REMARKS

Claims 1-12, 14-23, 25-35 and 37-47 are pending for further examination. Claims 1, 8-9, 20, 27-29, 32-33, 37-40, 42-45 and 47 are currently amended.

Examiner Interview

As a preliminary matter, Applicant thanks the Examiner and the Examiner's Supervisor for participating with the Applicant's representative in a telephone interview on October 22, 2007. No agreement was reached.

35 U.S.C. § 112 Rejections

The Office action rejected claims 37-39 and 42-44 as indefinite because the term "capable" is allegedly unclear. Applicant has amended claims 37-39 and 42-44 to address those rejections and respectfully requests reconsideration.

35 U.S.C. § 102 Rejections

Claims 1-3, 5, 13, 20-21, 23-26, 29, 31, 33, 35-37 and 40-43 were rejected under 35 U.S.C. § 102 as anticipated by Ekberg (U.S. Patent No. 7,003,282).

Claims 4, 6-12, 14-19, 22, 27-28, 30, 32, 34, 38-39 and 44-46 were rejected under 35 U.S.C. § 103 as unpatentable over the Ekberg patent.

In view of the foregoing amendments and the following remarks, Applicant respectfully requests reconsideration and withdrawal of the claim rejections.

Claim 1 (as amended) recites, in part, a method that includes generating a registration request message to have a home agent deliver datagrams, which are destined for a home address associated with a mobile device, to a second address on a network different from a home network. The method further includes producing an authentication message that contains a) authentication data encrypted with a first key and b) a data structure that includes the first key, in

which the data structure is encrypted with a second key. The authentication message containing the authentication data and data structure is embedded in the registration request message.

An example of the foregoing features is discussed in the present application on pages 5-6 and 9-11 and shown in FIG. 2. In that example, a mobile node 14, which has moved off of its home network into a foreign network, needs to register with its home agent so that any datagrams sent to its home address are rerouted to a care-of-address that the mobile node has obtained in the foreign network (*see* pg. 1, lines 7-10, 18-21; pg. 4, line 24 – pg. 5, line 8; pg. 10, lines 15-18). For that reason, the mobile node 14 generates (200) a Registration Request message, to be sent to the home agent, that includes the mobile node's care-of address (*see* pg. 10, lines 16-18). The mobile node 14 also generates (202) a Kerberos Application Request message that includes (a) an authenticator message encrypted with a mobile node-home agent session key and (b) a ticket for the home agent (*see* pg. 10, lines 18-21). The Kerberos Application request message is embedded (204) in the Registration Request message so that once the home agent receives the request, the home agent can authenticate that the device making the request is actually the mobile node (*see* pg. 5, line 22 – pg. 6, line 1; pg. 10, lines 21-23). By incorporating the authentication message as a part of the Registration Request, a secure method of authentication between the home agent and the mobile node is possible.

In contrast, there is no disclosure or suggestion in the Ekberg patent of a Registration Request message that includes an embedded "authentication message," in which the authentication message contains "authentication data encrypted with a first key" and a "data structure" encrypted with a second key.

The Ekberg patent discloses an authentication method in which a terminal in an IP network can be authenticated using the same subscriber identification information as in the user's mobile phone (*see* col. 2, lines 17-28; col. 5- col. 7). The Ekberg patent also discloses a method of providing a session key between two clients (A and B), in which each client may be a terminal that has already been authenticated (*see* col. 8, line 1 – col. 10, line 21). The key is used to encrypt data transmission that takes place between the two terminals (*see* col. 10, lines 19-21). As part of providing the session key, the Ekberg patent discloses that one of the terminals sends a

request for a session key to a security server (*see* col. 9, lines 51-59). The request includes: 1) a ticket $T_{c,tgs}$ that contains a connection specific key $K_{c,tgs}$, in which the ticket is encrypted with a second key K_{tgs} and 2) an authenticator Ac that is encrypted with the connection specific key $K_{c,tgs}$. The security server validates the information in the request and, if it is alright, the security server generates a session key that can be used to encrypt data transmission between the two clients.

The Office action alleges that the above request for a session key, as disclosed in the Ekberg patent, corresponds to the claimed "authentication message" that is embedded in a registration request message. That is incorrect. Although the Ekberg patent discloses sending a Registration Request message from a mobile terminal to a home agent, there is no disclosure or suggestion of "embedding" the session key request in the Registration Request. Instead, the session key request is generated after the Registration Request has already been sent from a mobile terminal to a home agent.

In particular, the Ekberg patent discloses that after a terminal has attached to a foreign network, it sends a Registration Request to its own home agent to register a care-of address. There is no disclosure or suggestion, however, that the session key request is "embedded" in the Registration Request message as alleged by the Office action. Instead, the session key request is generated *after* the Registration Request is sent. For example, the Ekberg patent discloses that, following the registration request, terminals A and B are authenticated by the security server (*see* col. 4, lines 54-64; col. 5, lines 3-12; col. 5, line 65 – col. 6, line 1) and that, once the security server "*has found* that the authentication was successful," the Kerberos protocol for providing a connection specific key will commence (*see* col. 8, lines 3-5, 17-21). Accordingly, if the session key request commences after authentication by the security server, and thus after the Registration Request is sent, it would not be possible to embed the session key request in the Registration Request, as alleged by the Office action. Instead, the Ekberg patent clearly discloses that the session key request is sent un-embedded from the terminal to the ticket-granting server, located within the security server (*see* col. 9, lines 60-61).

At least for the foregoing reason, claim 1 should be allowed.

Claims 2-12 and 14-19 depend from claim 1 and should be allowed for at least the same reason as claim 1.

Claim 20 recites, in part, a method that includes receiving at a home agent associated with a home network an authentication message embedded in a registration request message to reroute datagrams destined for a first address of a mobile device to a second address in which the request message contains a data structure having a first key encrypted with a second key.

As explained above regarding claim 1, there is no disclosure or suggestion in the Ekberg patent of a Registration Request message that includes an embedded authentication message.

At least for the foregoing reason, claim 20 should be allowed.

Claims 21-23 and 25-28 depend from claim 20 and should be allowed for at least the same reason as claim 20.

Claim 29 recites, in part, a computer program product that has instructions causing a processor to: 1) form an authentication message that contains authentication data encrypted with a first key and the first key encrypted with a second key; 2) generate a registration request message requesting that datagrams destined for a first address of a mobile device be routed to a second address; and 3) include the authentication request message in the registration request message.

As explained above regarding claim 1, there is no disclosure or suggestion in the Ekberg patent of a Registration Request message that includes the claimed authentication message.

At least for the foregoing reason, claim 29 should be allowed.

Claims 30-32 depend from claim 29 and should be allowed for at least the same reason as claim 29.

Claim 33 recites a computer program product that includes instruction causing a processor to extract an authentication message from a registration request message requesting that datagrams destined for a first address of a mobile device be routed to a second address, in

which the authentication message contains authentication data encrypted with a first key and a data structure comprising the first key, encrypted with a second key.

As set forth in reference to claim 1, the Ekberg patent fails to disclose or suggest extracting an authentication message from a registration request message as claimed.

At least for that reason, claim 33 should be allowed.

Claims 34-35 depend from claim 33 and should be allowed for at least the same reason as claim 33.

Claim 37 recites, in part, a system that includes a home agent associated with a first network and a second network device associated with the first network. The second network device is operable to produce an authentication message including a data structure comprising the first key with the data structure encrypted with a second key and generate a registration request message that includes the authentication message within the request message.

As discussed above in reference to claim 1, the Ekberg patent fails to disclose or suggest a registration request message that includes the authentication message as claimed.

At least for that reason, claim 37 should be allowed.

Claims 38-42 depend from claim 37 and should be allowed for at least the same reason as claim 37.

Claim 43 recites a system that includes a router associated with a home network and a processor operable to read a registration request message in which the registration request message contains a data structure including a first key unknown to the processor, encrypted with a second key that is known to the processor. The processor is also operable to verify an authentication message associated with the request message in which the authentication message includes a hashed version of the request message computed using the first key.

As discussed above in reference to claim 1, although the Ekberg patent discloses sending a Registration Request message to a home agent, there is no disclosure or suggestion that the request message includes a data structure having "a first key unknown to the processor,

encrypted with a second key that is known to the processor" as recited in pending claim 43. Instead, the ticket $T_{c,tgs}$, which the Office action alleges corresponds to the claimed data structure, is sent in an un-embedded session key request to a ticket granting server in the security server.

At least for the foregoing reason, claim 43 should be allowed.

Claims 44-47 depend from claim 43 and should be allowed for at least the same reason as claim 43.

It is believed that all of the pending claims have been addressed. However, the absence of a reply to a specific rejection, issue or comment does not signify agreement with or concession of that rejection, issue or comment. In addition, because the arguments made above may not be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

No fee is believed due. However, please apply any other charges or credits to deposit account 06-1050.

Respectfully submitted,

Date: November 1, 2007

/Samuel Borodach, Reg. No. 38,388/
Samuel Borodach
Reg. No. 38,388

Fish & Richardson P.C.
Citigroup Center
52nd Floor
153 East 53rd Street
New York, New York 10022-4611
Telephone: (212) 765-5070
Facsimile: (212) 258-2291